# Introduction to System Safety

Sandra L. Prior, REM, CHMM

System Safety and Safety Systems for Accelerators

US Particle Accelerator School

June 28 – July 2, 2004

# System Safety History

- System safety (SS) movement began in 1940s
  - Amos L. Wood, 14th Annual Meeting of the Institute of Aeronautical Sciences in January 1946
- USAF an early leader
- Air Force-Industry partnership began as early as 1954
- Early 60s, small group of managers, scientists, & engineers implemented SS in aerospace program
- In 1962, the System Safety Society was organized; professional organization in 1972

# What is System Safety?

System safety is the practice of proactive hazard management. It is based on the principle that, armed with sufficient knowledge, one can predict hazards associated with a process and can identify effective methods to lessen the risks associated with the hazards. System safety applies to the entire lifecycle of the process or thing that generates the hazard – from conception to decommissioning.

# USAF System Safety Definition

**Air Force System Safety Handbook:**

"The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system lifecycle."

# FAA System Safety Definition

**FAA System Safety Handbook:**

"The application of special technical and managerial skills to the systematic, *forward-looking* identification and control of hazards throughout the life cycle of a project, program, or activity."

# System Safety Principles

- Safety must be designed in.
- Inherent safety requires both engineering and management techniques to control the hazards.
- Safety requirements must be consistent with other program or design requirements.

# System Safety Goal

The goal of System Safety is to optimize safety by the identification of safety-related risks, eliminating or controlling them via design and/or procedures.

**Question- Where do you find the DOE system safety program defined?**

# DOE Safety Management System Policy 450.4

"The Department and Contractors must systematically integrate safety into management and work practices at all levels so that missions are accomplished while protecting the public, the workers, and the environment."

# Step 1: Define Objectives

- Typically documented in
  - Business Plan
  - Operating Specifications
- In what DOE document(s) might you find this type of information?

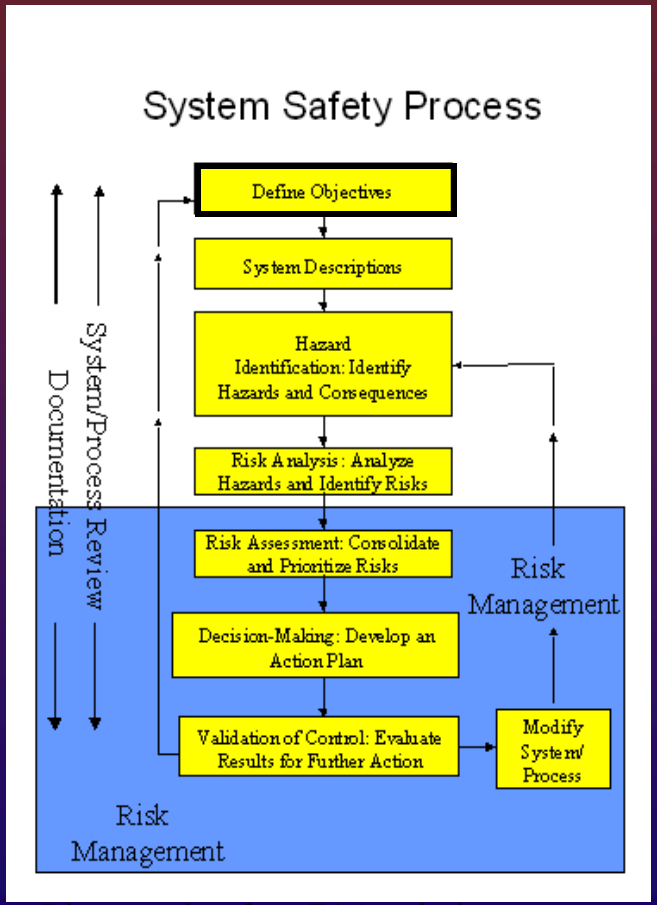


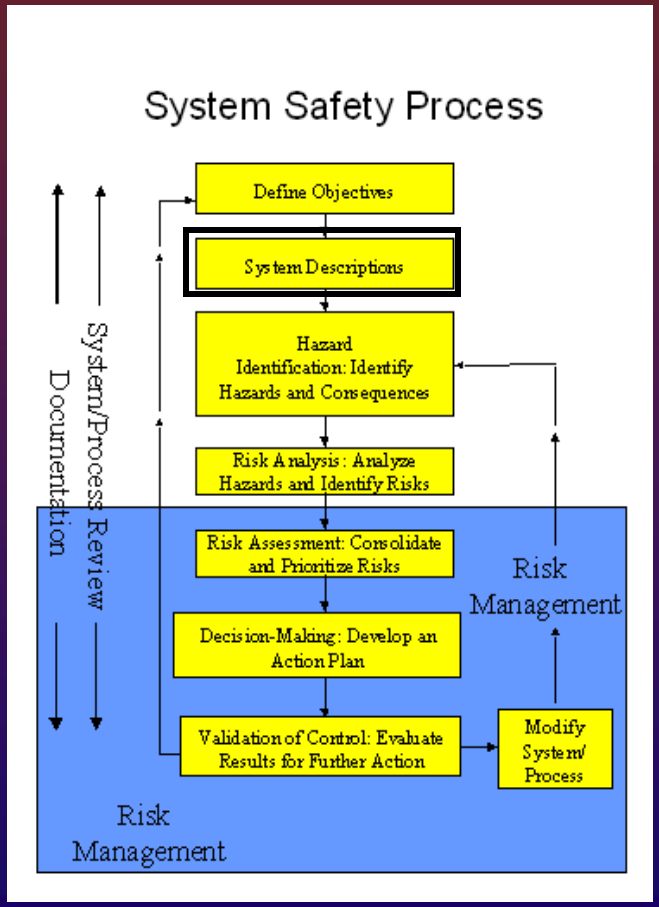

Diagram taken from FAA web site at http://www.asy.faa.gov/Risk/SSProcess/SSProcess.htm

“There are no "safety problems" in system planning or design. There are only engineering and/or management problems that, if left unresolved, may lead to accidents.”

FAA System Safety Handbook

# Step 2: System Description

- Provides a description of the interactions among:
  - People
  - Procedures
  - Tools
  - Materials
  - Equipment
  - Facilities
  - Software
  - Environment

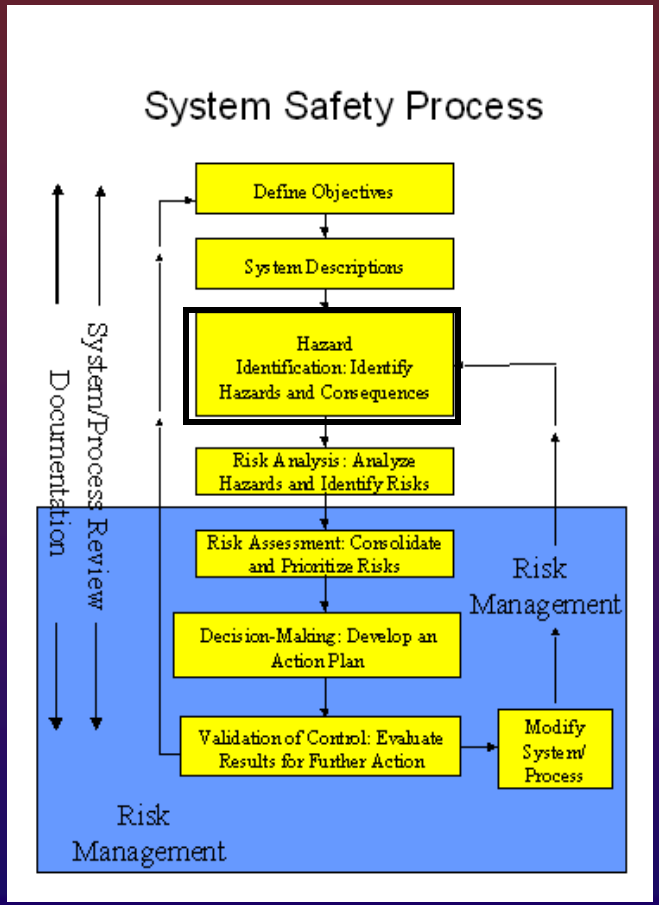


# System Description (continued)

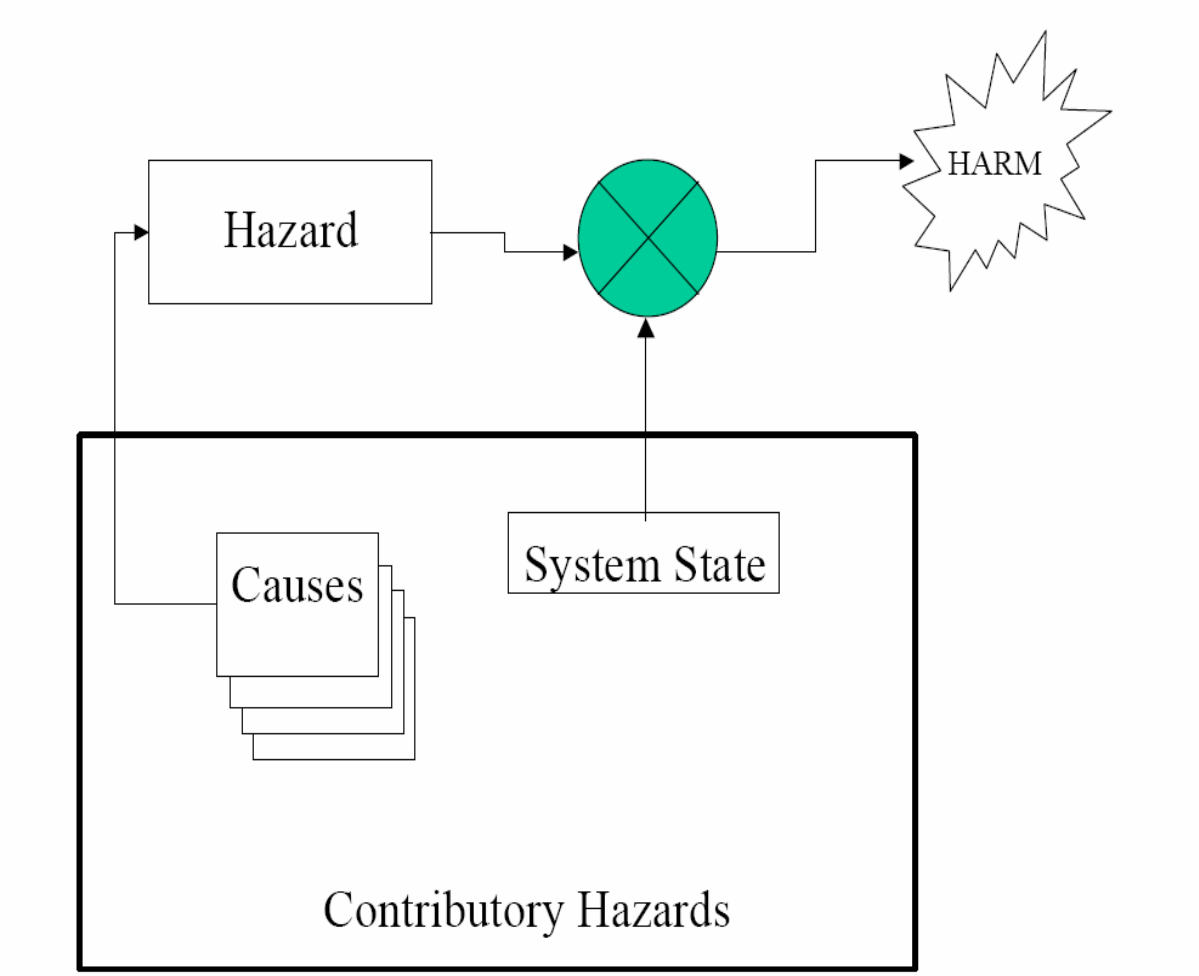
- **The object of a good system definition is to:**
  - ✓ **set limits for the following steps in the process**
  - ✓ **reduce complex systems into manageable parts.**

# Step 3: Hazard Identification

- Sources are both internal and external
- Preliminary Hazard List
- Group hazards by function
- Develop hazard scenarios
- Develop worst case scenarios



# Hazard Analysis

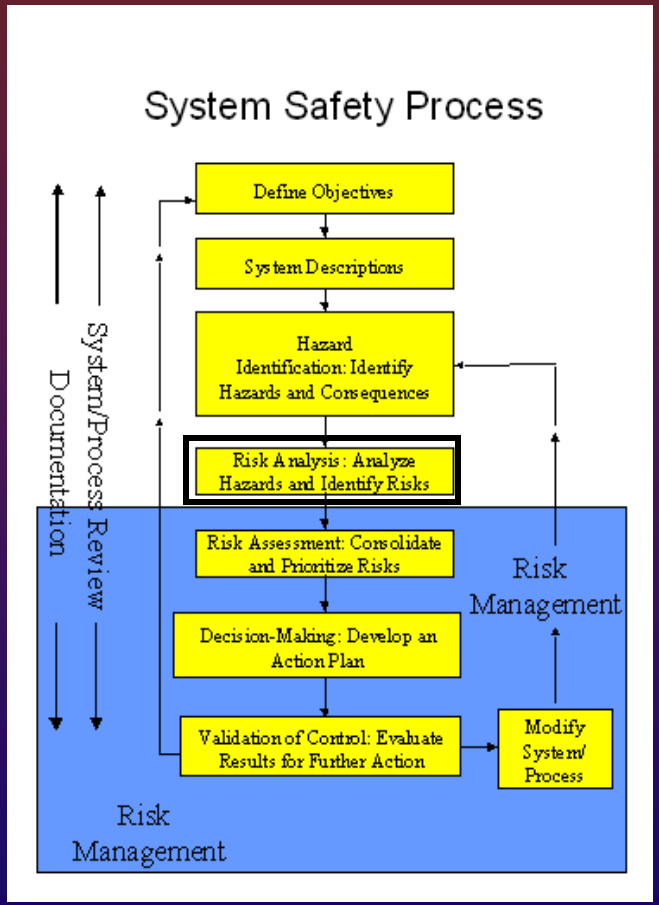



**Analysis should be:**

- ✓**Comprehensive**
- ✓**Methodical**
- ✓**Disciplined**

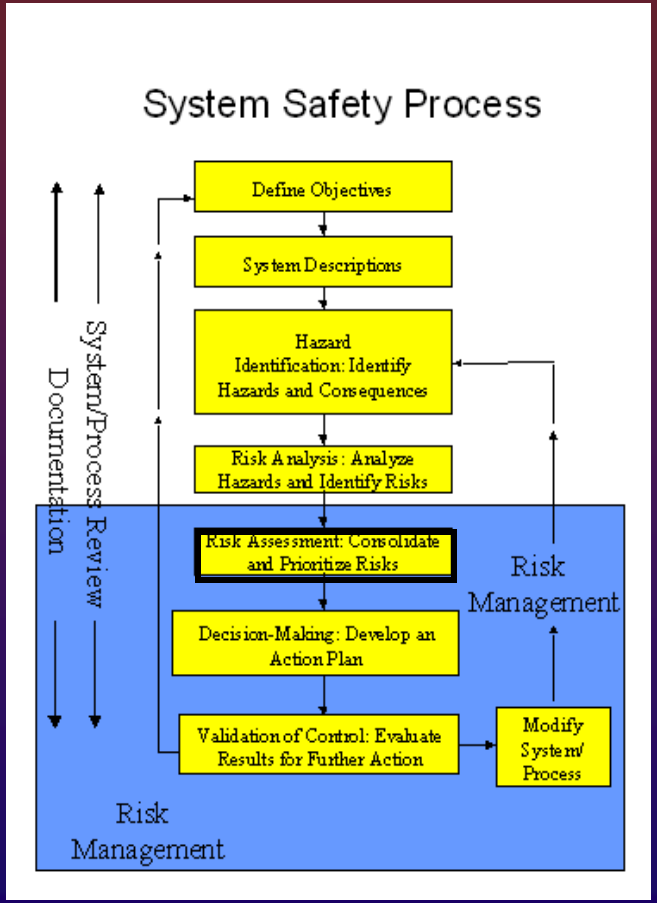
# Step 4: Risk Analysis

- Characterize hazards
  - Likelihood
  - severity
- Qualitative analysis
  - Matrix
  - PHA
  - What If/Checklist
  - Lessons Learned reports
- Quantitative analysis
  - FEMA



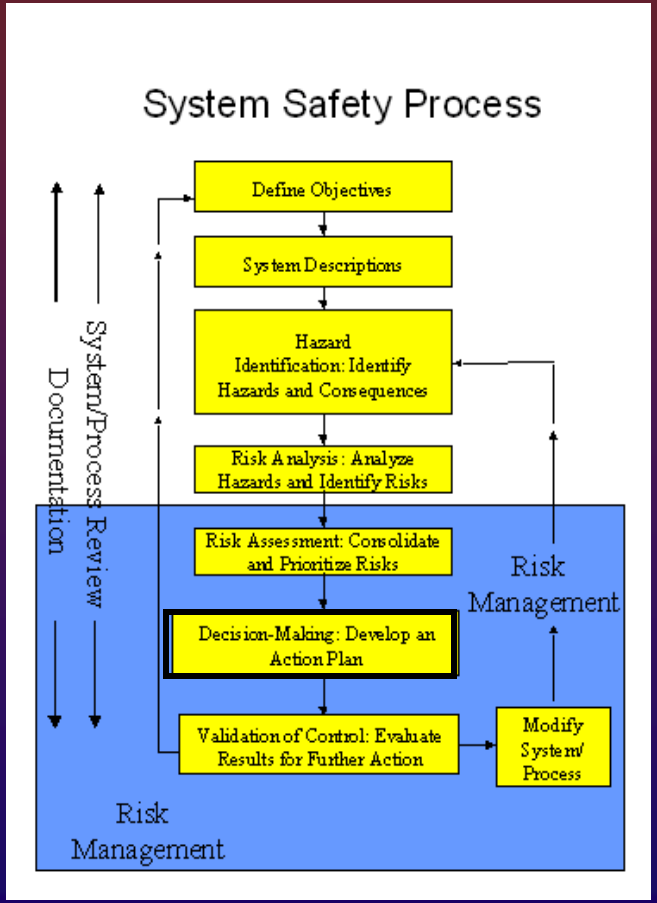
# Step 5: Risk Assessment

- Combine impacts of risk elements
- Compare impacts against acceptability criteria
- May consolidate risks into sets for joint mitigation and decision making



# Step 6: Decision Making

- Begins with
  - Management decision
  - Resources allocation
  - prioritized task list
- Most crucial step in process
- Decide how to address each risk
  - Safety Order of Precedence



# Safety Order of Precedence

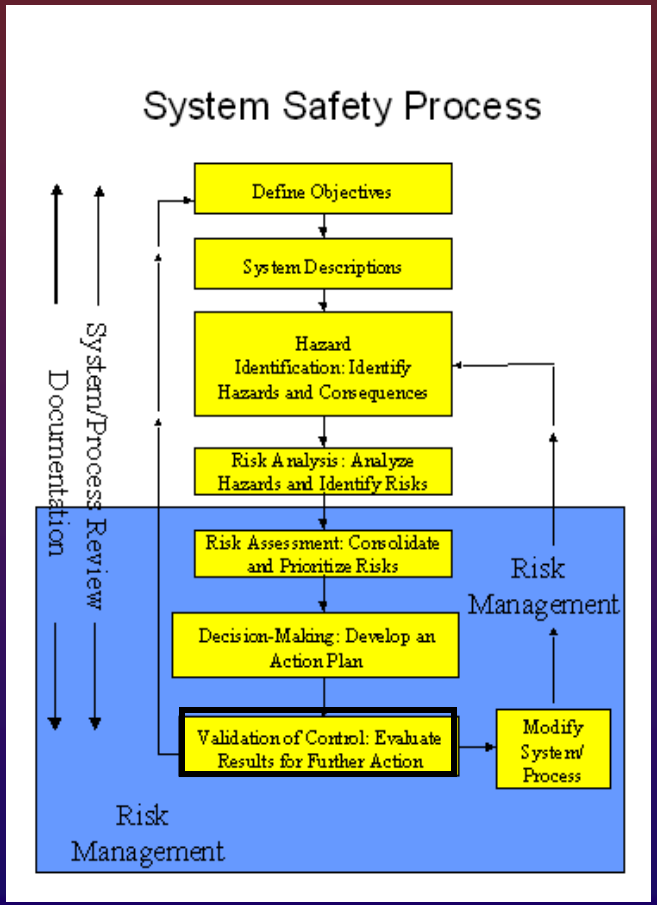
- Design engineering approach:
  - Design for minimum risk
  - Design to reduce hazards
  - Incorporate safety devices
  - Provide warning devices
  - Develop procedures and training
- Alternative action plans
- Final result -written assessment document

# Effective Safety Risk Management Decisions

- Assign qualified, competent personnel
- Authority commensurate w/ responsibility
- Define, document, & track all known hazards as program policy
- Include safety risk assessment in program reviews
  - Risk acceptability
  - Risk responsibility
  - Decision milestones

# Step 7: Validation & Control

- Analyze effectiveness
  - ID data collection needs
  - ID triggering events
  - Develop plan for data review
- Document each risk status
  - Acceptable
  - Unacceptable
  - unknown

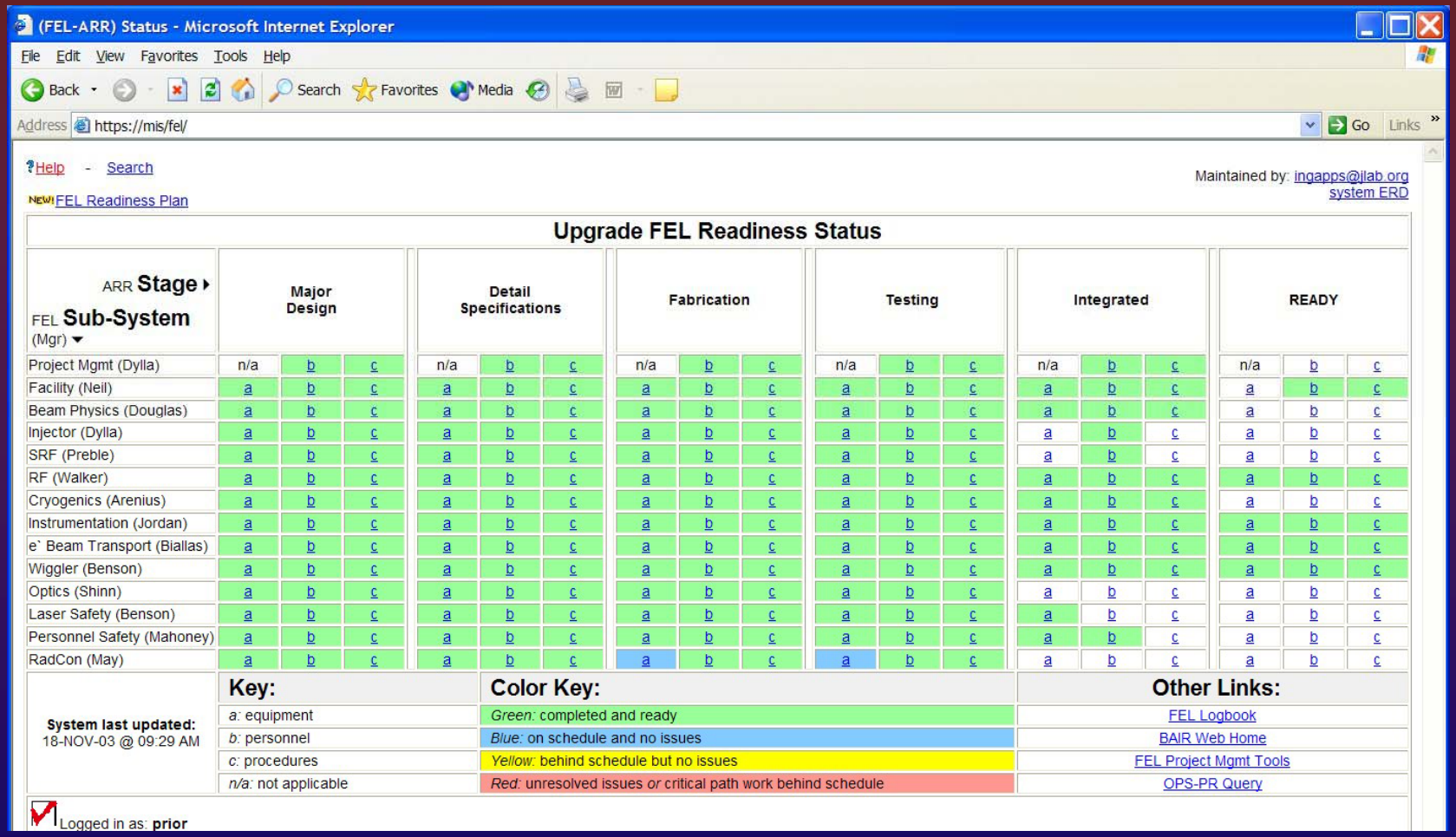


# DOE Accelerator Readiness Review (ARR)

- Required by DOE Order 420.2A, para 4.d –

  "Accelerator Readiness Reviews. Accelerator Readiness Reviews (ARRs) must be performed prior to approval for commissioning and routine operation and as directed by the Cognizant Secretarial Officer/NNSA Deputy Administrator or a field element manager/NNSA field manager."

# DOE Accelerator Readiness Review (ARR)



(FEL-ARR) Status - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address https://mis/fel/ Go Links

Help - Search

NEW! FEL Readiness Plan

Maintained by: ingapps@jlab.org
system ERD

**Upgrade FEL Readiness Status**

| ARR Stage ▸ / FEL Sub-System (Mgr) ▾ | Major Design | | | Detail Specifications | | | Fabrication | | | Testing | | | Integrated | | | READY | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Project Mgmt (Dylla) | n/a | b | c | n/a | b | c | n/a | b | c | n/a | b | c | n/a | b | c | n/a | b | c |
| Facility (Neil) | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c |
| Beam Physics (Douglas) | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c |
| Injector (Dylla) | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c |
| SRF (Preble) | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c |
| RF (Walker) | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c |
| Cryogenics (Arenius) | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c |
| Instrumentation (Jordan) | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c |
| e` Beam Transport (Biallas) | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c |
| Wiggler (Benson) | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c |
| Optics (Shinn) | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c |
| Laser Safety (Benson) | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c |
| Personnel Safety (Mahoney) | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c |
| RadCon (May) | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c | a | b | c |

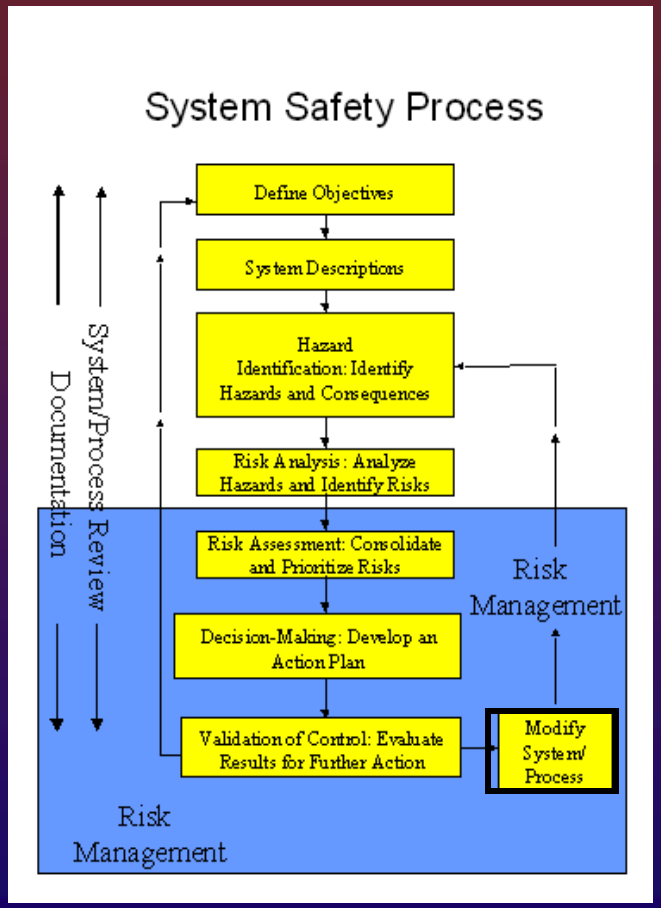
**System last updated:**
18-NOV-03 @ 09:29 AM

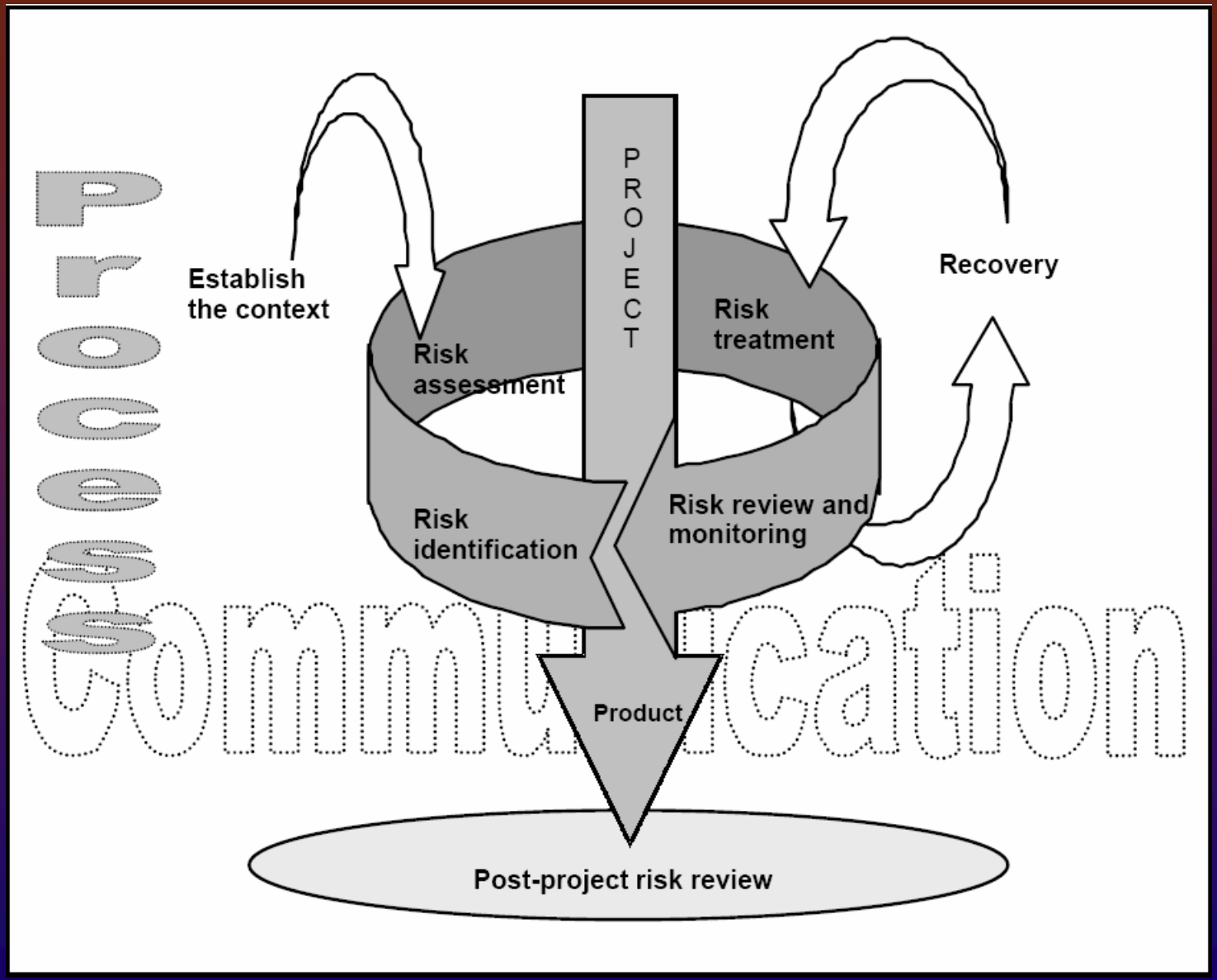
| Key: | Color Key: | Other Links: |
|---|---|---|
| *a:* equipment | *Green:* completed and ready | FEL Logbook |
| *b:* personnel | *Blue:* on schedule and no issues | BAIR Web Home |
| *c:* procedures | *Yellow:* behind schedule but no issues | FEL Project Mgmt Tools |
| *n/a:* not applicable | *Red:* unresolved issues *or* critical path work behind schedule | OPS-PR Query |

Logged in as: **prior**

# Step 8: Modify System/Process

- Modify if needed
- Why?
  - Risk status changes
  - Mitigation results are unacceptable
  - Addressed wrong hazard
  - System/process undergoes change
- Re-enter process at the hazard ID step





# Summary

- System Safety is a process that guides you into developing a context for your safety system design.
- The System Safety process requires you to document this context.
- Once your context has been established, you can then develop your safety system within that context.